International Journal of Information Technology and Knowledge Management
July-December 2010, Volume 2, No. 2, pp. 425-427

COMPUTER SECURITY: SELECTING AN EFFECTIVE BUSINESS SECURITY MODEL

Binod Kumar[1] & Kanak Saxena[2]

Individuals involved in e-business are often faced security problems, to protect their business information and data they need a security system. A reliable and effective security model provides best firewall and gateway configuration, and offers an encryption facility hard to detect. It also keeps balanced the system security and performance. This paper aim is to aware the business person from the impacts of various types of security theft; threats and attacks by discussing all aspects of security then assisting them to select an effective security model for their business.

Keywords: Firewall, Gateway, VPN, Implementation.

1. Introduction

Computer and Internet are playing vital role in each area of our life. It is not only playing roles in communication and entertainment but also in business in the form of E-Commerce.

It is helping us by processing, storing and transmitting huge data to desired place with no time. Application of Data Warehousing and Miming is supporting the business executives to take right decision and to get high return of investments.

Nowadays, entire globe become business market. Business is running around the clock and across the countries. In e-commerce the information and assets are moving in the form of text, graph, file, e-check and e-money which is of decision-making, money transaction, order confirmation and goods delivery on time.

An intruder can harm a businessman by intercepting and changing business moving data or can steal data from business server.

Hence to run a business smoothly business man needs a reliable security system that can protect corporate information and assets from intruders.

2. Security Problems and a Business Needs

[10] Security is a major concern at the top corporate, government, and academic levels of all sizes. Security problems in cyberspace are unlikely to disappear or be solved any time soon. [12] The external threats to computing devices are escalating and threats like worm and viruses multiply, the number of vulnerable devices proliferates, and wireless technologies provide more avenues of attack. [4] Networks are subjected to attack from packet snuffers, IP spoofing, denial of service (DoS), spam, viruses, worms, Trojan horses, and a host of other threats. The IT Act-2000 and its Section 43A, 43G, 66(1), 66(2) and 67 seems helpless to stop the thefts.

No any security systems remained applicable for long time. These were broken and information was theft. Especially in net banking, it happened frequently. Protecting corporate information and technology assets from intruders, thieves, and venders is still a significant challenge for enterprises.

These forces are driving organizations to seek more fundamental and broad-based security solutions that ensure privacy, data integrity, user authentication, and access control at the server, the client, and across the network.

3. Security Threats, Thefts and Attacks Overview

(i) Instant Messaging (IM): Messaging products like MSN, Yahoo, AOL etc are used today as a business communication tool. Effects- emphasizes functionality over security and placing enterprise systems at risk to hackers, viruses, worms, Trojans and violation of privacy laws.

(ii) Phishing and Electronic Identity Theft: Mass e-mailing sent by phishers, looks as sent by banks, mortgage companies, brokerage firms or other legitimate organizations with which the recipients may do business. Effects- get divulge information like account id and passwords.

(iii) Malware: Abbreviation for malicious software. It

[1]Asst. Prof. & HOD, MCA, LNCTS, Raisen Road, Kalchuri Nagar, Bhopal(M.P.)-462021

[2]SATI, Vidisha (M.P.)

Email: [1]binodkr75@gmail.com, [2]ksv1909@yahoo.com

refers programs like Trojan horse, spyware and adware that perform unwanted actions get installed without the user's permission. Effects- changes settings of a modem's dialup connection so that it will call a number.

(iv) Viruses and Worms: Small unwanted programs that replicate themselves and spread through e-mail, HTML mail, P2P file sharing, instant messages, files downloaded from Web sites, FTP sites, newsgroups, or other sources. It may lie dormant until a particular date or time or specific circumstances trigger them. Effects- damage files, crashing programs, or flooding networks with so much traffic.

(v) Trojan Horses: Malicious programs that disguised as legitimate software often installed along with free software. Effects-perform malicious action, create a back door for hackers and send sensitive information to the hacker.

(vi) Adware and Spyware: Software products display advertising, installed along with another downloaded program. Effects- Changes browser's home page collects and transmits information.

(vii) Cookies: Text files placed on computer by Web sites to retain information we have entered on the site. Effects- track Web activities and target advertising to us based on our activities.

(viii) Password Cracking: Password cracking method based on commonly used passwords or personal information about the user, such as the name of a spouse, child, or pet, or a social security or phone number. Other methods are dictionary attacks, brute force attacks and social engineering. Effects- enable outsiders to work as an authorized user/ administrator.

(ix) Hack Attacks: Specific attacks used to gain access or bring down a computer system or network. Effects- Intercepts messages and then modify it. Crash a system or take control of it.

(x) Denial of Service Attacks: Involves flooding a system or network with more data than it can handle. Example Buffer overflow, SYN flood, Teardrop attack and Smurf attack. Effects- System crashes or network bandwidth is so clogged.

(xi) Spoofing: A mechanism used by attackers to disguise the origin of an attack. Examples are IP, E-mail and Web spoofing. Effects- It enables to disguise the origin of an attack.

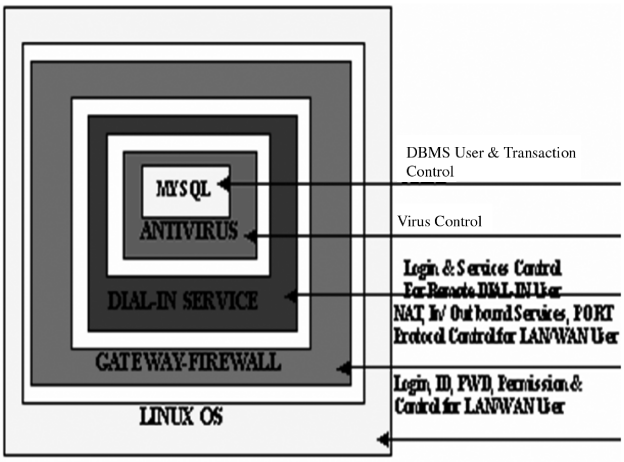
(xii) Port Scanning: A port is a logical point of connection that is used by network applications for communications between two computers. Effects- Enables attackers to enter into system through an open port.

4. SELECTING AN EFFECTIVE SECURITY SYSTEM

To select an effective security model some discussion need to do in the field of Authentication, Access Control, Confidentiality, Integrity, and its availability. Security model design need to analysis by angles from the evolved form of one or more of these fields of ciphering [9] i.e. ECB, CBC, CFB & OFB; Authentications i.e. User & Client; Access Control i.e. Firewall, Intrusions Detection System, Virus Detection System; Integrity i.e. Logging and Auditing, Public Key, Private key, Digital Signature [3]; and Confidentiality i.e. VPN, NAT, [7] Gateway.

[8] The aim of model must be to control and minimize damage, preserve evidence, quick and efficient recovery, and gain insight into threats against the organization.

To achieve task of Authentication, Confidentiality and Integrity with best way, cryptography techniques like DES, SKIPJACK, Triple DES, IDEA, RCA4/128 and Digital Signature & Certificate can be used, best configuration of firewall VPN and gateway can be advised to achieve task of Access control, and protocols like SET, S/MIME, and SSL can be used to provide best data security and privacy over Internet.



[5] Best practices begin with a layered defense at the gateway and desktop levels. The layered approach is both a technical strategy, espousing adequate measures be put in place at different levels within the network infrastructure, and an organizational strategy requiring buy-in and participation from the board of directors down to the shop floor. Cisco system and its partner has offered a complete array of multi-tiered solutions to provide robust protection to every portion of the data infrastructure, from the network core to desktops and remote sites, and every point in between, to enable business to expand their e-business initiatives with confidence. [11] To manage communication

security key challenge one solution called SSH client/sever, provides end-to-end secure communication within a corporate network.

[1] SSL VPN technology is designed specifically to enable increased productivity for remote users by providing easy-to-use, secure access to applications and resources on your networks, while minimizing many associated risks and significantly lowering administration and support costs. [2] VPN enables two or more networks connect to each other over a public network, securely. [6] SSL VPN has emerged as a way to enable employees and business partners anywhere access from Corporate owned PCs to airport kiosks.

5. CONCLUSION

The security thefts, threats and attacks are major problems for computer and Internet based business. Many managers and users of this area find it difficult to keep their information and IT assets safe and secure. In order to assist with this, the Department of computer science and Information Technology contribute their knowledge of secure transmission, exchange, transfer and management of business information and assets.

REFERENCES

[1] Aventail Corporation. SSL VPN Technical Primer, March 2006.

[2] Alok Sinha. Implementing VPN in Linux: Setup a Complete VPN Solution in Linux, 30 January 2006.

[3] Andrew S. Tanenbaum. Computer Networks: Digital Signatures, Fourth Edition, Prentice Hall of India Pvt. Ltd., New Delhi-110001.

[4] Cisco System. SMB Class Security Solutions: Technical and Business Advantages of Cisco Security Solutions, November 2005.

[5] CP Secure, Inc. Stopping Spyware at the Internet Gateway: Lessons from Real Word Spyware, Jan/Feb 2006.

[6] Check Pint Software Tech. Inc. SSL, VPN A Practical Solution for Secure Remote Access Anywhere Anytime, March 2006.

[7] Christopher Negus. Red hat Rel 12 Bible: Gateways and NAT, Edition 2005, Wiley Publishing Inc., USA.

[8] Georgia Killcrece, Klaus-Peter Kossakowskl, Robin Ruefle, Mark Zajicek.Organisational Models for Computter Security Incident Response Teams (CSIRTs), Dec 2003.

[9] Harish B, P V Bhandari. Secured e-Commerce Transaction, Manipal Academy of Higher Education, Manipal-576119.

[10] Sandhu R. "IEEE Internet Computing", IEEE. 7, Issue 6, Page(s):45 – 52, J Nov.-Dec. 2003.

[11] Swapnil Arora. "Secure Communication through SSH", PCQuest Magazine, June 2006.

[12] Trusted Computing Group Administration. "The Trusted Computing Platform Emerges as Industry's First Comprehensive Approach to IT Security", Security '02, Feb 2006.